accenture

Ransomware in the Health Industry

Resiliency and Response

Recording Transcript

Patty Enrado: Hi. I'm Patty Enrado, and today I'm with Salwa Rafee, global managing director for Healthcare Security, and Cesar Villalta, managing director, global security lead for Life Sciences, both for Accenture. Welcome, Salwa and Cesar.

Salwa Rafee: Thank you very much, Patty, for having us.

Cesar Villalta: Yes. Thank you, Patty.

Patty: For today's podcast, we're going to talk about resiliency in response to ransomware in the health industry. Let's first talk about why ransomware is becoming an increasing threat to health organizations. Salwa, why should health organizations care about the threat of ransomware?

Salwa: Patty, they should care very much about ransomware and all kinds of cyberattacks. This is an existential threat to our industry. Healthcare organizations are the most vulnerable compared even to other industries for many reasons we will talk about later. But simply put, when a ransomware attack happens, hospitals, HDOs, and the insurance industry will just stop serving patients, which is the bread and butter of our business. This is why hospitals exist, to serve our patients. So, it is stopping all the operations. We can't retrieve patient data, we can't resume treatment and diagnosis. As I said, it's an existential threat, and we should all worry about that.

Patty: Salwa, can you give an example of the impacts that ransomware attacks have had on the health ecosystem?

Salwa: Absolutely. We have seen many examples of hospitals and even payer organizations being attacked. When that happens, data, the most precious assets across all industries, are being exposed.

This is a huge patient safety issue. It stops the day-to-day business of the healthcare organizations from opening their doors to receive patients, resume their treatment plans, and perform diagnostic procedures, operations, and surgeries. So, the loss of data, the loss of operations, and the loss of branding and reputation of these organizations—these are critical for our industry.

Patty: How has the threat of ransomware evolved over the past year?

Salwa: It has evolved exponentially. Within a couple of years, with a global pandemic, we know that digitization has happened in healthcare in a very speedy way. There was a race to research, a race to find a cure, and the vaccine for COVID. It was very impressive to achieve these kinds of results in a very short period, but that progress has been paired with the extreme threat of cyberattacks. Very sophisticated actors were targeting healthcare organizations for very good reasons, frankly. To steal the data, to stop the operations, to extort all kinds of ransom from the organizations. As you know, the industry is most vulnerable because of the spending and the use of legacy infrastructure. Many reasons make our organizations vulnerable, and we need to change that.

Patty: Are we seeing any governmental action in reaction to these threats?

Salwa: Absolutely. I know that you might remember in the last couple of months there has been an executive order from the White House on cybersecurity, and the mandate for everybody to share threat intelligence, to share incidents, to develop recommendations for what happens as an incident response plan. So, there is a national effort to make our defense systems proactive and how to respond to a cyberattack with this White House executive order. Many great outcomes have come out of it. And I think all organizations have more awareness now of this threat. Sometimes when I talk to our clients, I tell them it's not an "if," it's a "when" they will have a cyberattack, especially a ransomware attack. It's inevitable. We can't inadvertently help the bad actors to attack our industries. It's how we act that will define our response and protect our business.

Patty: Let's focus on the typical challenges that health organizations face in preparing and responding to ransomware attacks. Cesar, what are typical challenges that they encounter when preparing and responding to ransomware attacks?

Cesar: Ransomware has certainly become top of mind for many organizations, including in the healthcare and life sciences industries. And access to ransomware, specifically as a service, has increased and is available to the masses.

What that means is that almost anybody, if they're looking for it, can gain access to ransomware software, if they're willing to pay. When healthcare organizations are thinking about this and preparing, there are a few things that they should focus on. And we'll talk a little bit about this in greater detail.

First, business continuity. That's kind of the fundamental, getting back to the basics, but understanding that, having a complete, valid, offline backup to critical systems and data is mission-critical and extremely important. Next, understanding hygiene and making sure that we're being proactive here. And in many instances, when you look into the origination around ransomware, you're looking at kind of a lack of hygiene.

It's not about having an agent on an endpoint, it's ensuring it's continuously updated, it's healthy, and in fact, protecting against the latest threats. And then ultimately spending time and focusing to test these defenses. Adversaries are continuously testing our defenses, we should be looking to do this more than just once or twice a year, and embedding it in the way we work. I think it means having a holistic approach and holistic thoughts behind this that would help in preparing and responding to ransomware.

Patty: So, most ransomware attacks start with cyber hygiene issues and human mistakes. Why is this the case?

Cesar: It's a path of least resistance. You know, cybersecurity is a combination of people, processes, and technology. And the people part has typically been the most exploited part when it comes to phishing, when it comes to remaining cyber vigilant. You know, when we look at the pandemic way of working, the world that we've been in for going on two years now. Individual lives have become blurred between home and work. It's all kind of one state of being. As a result, mistakes happen. Remaining cyber vigilant at home versus work is a tough line to walk. It's important to understand that technology. Hygiene in terms of the health of your security defenses is important. But your people also need to understand and operate with a heightened sense of hygiene in that cyber-vigilant aspect so that the entire package comes together to protect your organization.

Patty: The health ecosystem is known for its large level of interdependency across the supply chain. So how does this affect the risk of ransomware attacks?

Cesar: Patty, this is a good one. At the end of the day, it certainly amplifies the risk. You know, Salwa and I work together at Accenture to protect our clients across the entire health value chain, from drug manufacturing through the delivery of patient care. And the reality is, this entire value chain is highly interdependent and highly connected.

There have been several examples where an organization may have the best defenses or reasonable defenses in place, but a partner, whether it's a processing partner, a technology partner, or a delivery partner, has become compromised. That attack directly impacts the entity, even if it doesn't involve their direct operational functionality. Unfortunately, it only takes one kind of disruption in your critical supply chain to disrupt your business. It's highly connected, highly interdependent at this point. The goal isn't just to protect what's inside your defenses, but rather to have a comprehensive plan throughout your ecosystem of partners to ensure that you minimize the risk of ransomware and business disruption.

Patty: Let's look at how to increase business resilience against ransomware attacks. Salwa, what should all health organizations do right away to increase their resiliency against ransomware attacks?

Salwa: That's a great question, Patty. You can't protect what you cannot see. The first thing is for them to immediately do a security assessment of the entire infrastructure, networking, IoT, IUMT, applications, data, everything. Usually, this assessment offers great findings and insights about the gaps and the vulnerabilities in any organization. From that, you can take action to protect, remediate, and strengthen your posture when it comes to your defense system against cyberattacks.

I would recommend every single organization do this assessment on an annual basis at least. Once we know that it gives us greater freedom to immediately start to strengthen that system.

It's important to be proactive, but also to know how to respond and build a very comprehensive, holistic approach for incident response. You need a crisis management approach to what happens if the organization has been attacked with ransomware: what to do with the data, how to make sure backup data are saved and can be used—all these aspects. It gets into greater detail, but there are so many different action plans that will be recommended based on this assessment and the visibility.

Patty: Salwa, how can organizations build a human firewall to protect against ransomware attacks?

Salwa: This starts with cyber hygiene and cyber awareness. Humans are the weakest points. When you are a nurse in a hospital or a user, they are receiving 20 emails per hour, you will want to get through your emails very quickly. And with that, sometimes—most of the time—there are phishing email messages you don't pay attention to, and you press on this link, this hotlink, to see if you must change your password, or if there is something important coming from your boss. And this is the entry point to most ransomware attacks.

You know, the hackers get into your system and move laterally, if they steal your credentials, and then move upward for more privileged access. So, cyber awareness, continuous training, continuous programs. Making sure that everybody is vigilant against all these cyber-attacks. A human firewall is our first line of defense, and then we can strengthen and harden the other parts of the technology and the tools.

Patty: Cesar, what actions would you recommend to validate and test measures that organizations have put into place?

Cesar: This is a good one, Patty. As Salwa mentioned earlier, having an incident response plan is certainly important. It's important to exercise that plan. It's important to factor in the outcomes of your security assessments and continuously improve that plan. I'd recommend, if possible, don't go it alone. Find a partner that can help you independently think about the critical path to that plan, who can help you "pressure test." Bring in what peers are doing in the industry to optimize and drive an effective outcome with the plan. And then the testing aspect is going to be important. Again, it's not a one-time event. Our adversaries, third-party actors, are continuously testing our defenses, and we should be thinking about it that same way.

Patty: How should an organization prepare if it does fall victim to a ransomware attack?

Cesar: I mentioned the concept of don't go it alone. Organizations often learn during an event that they should have either retained an incident response partner or thought about securing outside help in the case of an emergency. When you're in the moment, it's too late to call for help. You certainly can do that, but you need the ability to call on a partner that has experience in dealing with these types of events. I'd also encourage organizations to treat this not just as a security event, but as an overall business disruption crisis event. It has become that important, especially in the healthcare industry. You know, down systems are one thing, but disrupting the ability to provide patient care is another. I think it's important to elevate these types of events in the right way within an organization.

The other thing to think about here is preparation, so CISA, the Cybersecurity Infrastructure Security Agency, has provided some guidance concerning ransomware; things to do, things to consider. I'd certainly encourage organizations to look at that guidance, subscribe to those alerts, if they aren't already. But there is some good thinking there around being proactive and how to remain calm during the storm, that I would recommend to organizations.

Patty: My last question to you: Should organizations ever consider just paying the ransom if they do fall victim to an attack?

Cesar: This is a controversial question and I welcome Salwa's perspective, too. I haven't met a cybersecurity practitioner yet that said yes. I think if the decision were up to a cyber organization or a cyber leader, we would typically default to no. Because by paying the ransom, you set yourself up for potentially being the target of either the same threat actor or a different threat actor. You also fuel the fire around this issue and enable these organizations to do this same thing elsewhere.

Typically, the decision to pay is more of a business function. How do you restore a state of operations as quickly as possible? If you remain resilient and can recover in a meaningful way, in a timely way, then the answer should remain no. But at the end of the day, this is more of a business decision, and it's a tough one.

Salwa: I completely agree with Caesar. It is an executive decision. The board of directors will have to make this decision on behalf of the organization. And in some instances, you know, you don't want to pay the cyber actors because it's like paying a terrorist organization. And the DHS frowns on that. It could lead to major repercussions. However, we in Accenture cannot recommend a yes or a no—it's up to the organization. We hope they do not have to make this decision. And it is our duty and mandate to make sure they are never in this kind of a situation that they must think about that. So, I hope that answers your question, Patty.

Patty: Salwa and Cesar, both of you said some great things. I want to boil things down to a few takeaways for our listeners. I think the operative word is “continuously.” Salwa, as you said, doing the annual security assessment, a holistic one, of all your systems, all your data. Once you do that assessment, you find those gaps, you have insights into what you need to strengthen; where are the weak parts, and have an incident response crisis management plan. Then there is continuous training. It's not a one-and-done, you train and that's it, but, again, the word continuous. Continuous training.

Cesar, you talked about having a trusted partner to help you validate and test, one that has best practices that it can share with the organization. So, again, continuously validating and testing, having that partner to help you. So, Cesar and Salwa, is there anything else that you want to add to that?

Salwa: I'd quickly add that, keeping in mind that cybersecurity, especially in healthcare, enables all our technology usage and deployment. It is an enabler for innovation. And sometimes we forget that part that we think is an add-on or just an added cost to spend on security solutions. But at the end of the day, it pushes for innovation, data protection, patient safety, and our privacy. We are all patients at some point in time, and we care about our well-being, our families, our citizens.

So, security is an intrinsic part of all our practices, frankly, across all industries, but has a very special meaning when it comes to the big H, healthcare, and life sciences.

Cesar: I couldn't have said it better, I 100% agree with Salwa.

Salwa: Thank you, Cesar.

Patty: Great. Well, thank you so much for your time, Salwa and Cesar.

Salwa: Take care.

Cesar: Thanks, Patty.